



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of: **Matthias ERNST, et al.**

Art Unit: **1640**

Application Number: **10/539,506**

Examiner: **Trang T. Doan**

Filed: **January 10, 2006**

Confirmation Number: **4654**

For: **AUTOMATIC, CONNECTION-BASED TERMINAL OR USER
AUTHENTICATION IN COMMUNICATION NETWORKS**

Attorney Docket Number: **052703**
Customer Number: **38834**

SUBMISSION OF APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

May 7, 2008

Sir:

Applicants submit herewith an Appeal Brief in the above-identified U.S. patent application.

Attached please find a check in the amount of \$510.00 to cover the cost for the Appeal Brief. If any additional fees are due in connection with this submission, please charge Deposit Account No. 50-2866.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

A handwritten signature in black ink that appears to read "William M. Schertler".

William M. Schertler
Attorney for Appellants
Registration No. 35,348
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

WMS/dlt



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL BRIEF FOR THE APPELLANT

Ex parte Matthias ERNST et al. (Appellants)

AUTOMATIC, CONNECTION-BASED TERMINAL OR USER AUTHENTICATION IN
COMMUNICATION NETWORKS

Application Number: 10/539,506

Filed: January 10, 2006

Appeal No.:

Art Unit: 1640

Examiner: Trang T. Doan

Submitted by:
William M. Schertler
Registration No. 35,348
Attorney for Appellants

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 Connecticut Avenue NW, Suite 700
Washington, D.C. 20036
Tel (202) 822-1100
Fax (202) 822-1111

May 7, 2008

BRIEF ON APPEAL

(I) REAL PARTY IN INTEREST

The real party in interest is **BT (GERMANY) GmbH & CO. OHG**, by an assignment recorded in the U. S. Patent and Trademark Office on April 13, 2006, at Reel 017465, Frame 0171.

(II) RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to appellant, appellant's legal representative, or assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(III) STATUS OF CLAIMS

Pending claims 1-23 stand rejected. No claims have been allowed, objected to, withdrawn or cancelled. The claims on appeal are claims 1-23.

(IV) STATUS OF AMENDMENTS

No amendments were filed subsequent to the final rejection.

05/08/2008 MGBREN1 02828052 10539586

02 FC:1402

510.00 OP

(V) SUMMARY OF THE CLAIMED SUBJECT MATTER

There are two (2) independent claims pending in this application, claims 1 and 16.

Claim 1

The invention recited in claim 1 is a method for automatically identifying an access right to protected areas in a first network (e.g., system of network provider 2 in Fig. 1; see, e.g., page 2, lines 16-17 and page 7, line 11 of appellants' specification) using a unique connection identifier (see, e.g., page 3, lines 20-21; page 7, lines 13-15 and page 8, lines 11-18 of appellants' specification) of a second network (e.g., telecommunications network 1 in Fig. 1; see, e.g., page 7, lines 9-10 of appellants' specification), comprising the following procedural steps:

dynamic or static assignment of a unique identifier of the first network for a terminal (see, e.g., page 5, lines 15-16 of appellants' specification), during or prior to the latter's connection to the first network by means of the second network (see, e.g., page 2, lines 21-22 and page 3, lines 15-19 of appellants' specification);

storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit (e.g., authentication unit 16 in Fig. 1; see, e.g., page 2, lines 22-23; and page 8, lines 6-8 and 13-16 of appellants' specification);

a provider of the protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area (see, e.g., page 2, line 24-page 3, line 2 and page 8, lines 20-25 of appellants' specification);

authenticating the unique connection identifier of the second network and/or communicating the unique connection identifier of the second network to the provider of the

protected area by means of the authentication unit (see, e.g., page 8, line 25-page 9, line 2 and page 9, lines 13-15 of appellants' specification); and

checking whether an access right for the protected area exists for the unique connection identifier of the second network (see, e.g., col. 3, lines 2-3 of appellants' specification).

Claim 16

The invention recited in claim 16 is a method for providing data for automatic identification of access rights to protected areas in networks (see, e.g., page 5, lines 3-5 of appellants' specification), comprising the following procedural steps:

provision of at least one unique identifier respectively from at least two different networks while a connection to both networks exists, whereby the connection to one of the networks happens by means of the other network (see, e.g., page 5, lines 5-6 of appellants' specification);

storage of a combination of the unique identifiers in an authentication unit (see, e.g., page 5, line 7 of appellants' specification);

authenticating and/or issuing of one of the unique identifiers when a corresponding enquiry is made regarding an other of the unique identifiers (see, e.g., page 5, lines 7-9 of appellants' specification); and

deletion of data from the authentication unit as soon as a connection with at least one of the two networks has ended (see, e.g., page 5, lines 9-10 of appellants' specification).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellants appeal the final refection of claims 1-23 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Publication No. 2003/0169714 to **Nakajima** (hereinafter “**Nakajima**”).

(VII) ARGUMENT

Appellants explain hereinbelow why the claim rejection should be reversed.

The rejection of claims 1-23 under 35 U.S.C. §102(e) as being anticipated by Nakajima should be reversed

As will be discussed in detail below, appellants submit that the **Nakajima** reference does not anticipate the claimed invention under §102 and, as such, the rejection of claims 1-23 should be reversed. More specifically, Examiner has not established anticipation under §102 because the **Nakajima** reference does not disclose all claimed method steps recited in independent claims 1 and 16.

Anticipation under §102 is established *only* if *all the elements* of an invention, as stated in the claim, are identically set forth in *a single* prior art reference. Moreover, it is not sufficient that each element be found somewhere in the reference, the elements must be “*arranged as in the claim.*” *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 703 F.2d 1452, 1458 (Fed.Cir. 1984).

The Nakajima reference does not disclose all elements recited in claim 1

Independent claim 1, and claims 2-15 and 22-23 which depend therefrom, are argued as a group with respect to this argument

Initially, to help facilitate a better understanding of the present invention and the claimed subject matter, an example of the operation an embodiment of the present invention will be discussed below. The example discussed below relates to accessing a service on the Internet via a telephone connection. For example, the Internet may correspond to the “first network” recited in claim 1, in which a typical “unique identifier of the first network” may be the IP (Internet Protocol) address. For example, the telephone network may correspond to the “second network” recited in claim 1, and, for example, a typical “unique connection identifier” of the second network may be a telephone number.

During or prior to connecting to the first network (i.e., Internet) by means of the second network (i.e., telephone network), the unique identifier of the first network (i.e., IP address) is dynamically or statically assigned to a terminal connecting to the first network (Internet) by means of the second network (telephone). Then, a combination of at least the unique connection identifier (telephone number) of the second network by means of which the connection to the first network (Internet) was made, and the unique identifier of the first network (IP address) are stored in an authentication unit. A provider of a protected area in the first network (Internet) requests the authentication unit to determine the unique connection identifier (telephone number) of the second network using the unique identifier (IP address) of the first network (Internet) when the terminal would like to access the protected area.

The features of the invention discussed above allow a terminal to access protected areas in the first network (Internet), such as a pay TV channel, etc., after connecting to the first network and after an authentication request is issued to the authentication unit by the service provider.

Nakajima does not disclose or suggest the claimed "a provider of the protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area," recited in claim 1

In the final Office Action dated August 8, 2007, the Examiner asserts the following correspondence between the claimed elements and the Nakajima disclosure: (1) the Internet 104 (Fig. 2) corresponds to the claimed “first network”; (2) a mobile communication network 100 (Fig. 2) corresponds to the claimed “second network”; (3) a telephone number of a mobile terminal 105 (Fig. 2) corresponds to the claimed “unique connection identifier of the second network”; and (4) the IP address for accessing the Internet 104 via the service gateway 102 corresponds to the claimed “unique identifier of the first network.” See, e.g., final Office Action, page 2, lines 10-16 and page 3, lines 8-12.

Further, in the Advisory Action dated December 27, 2007, the Examiner addresses the claim recitation “*a provider of the protected area requesting ... when the terminal would like access to the protected area,*” and asserts that the following supports Nakajima’s teaching of this claimed feature:

Examiner notes, on page 3 paragraph 0037, Nakajima discloses a situation where a mobile terminal transmits a service request (i.e., accessing the Internet, a wireless LAN, or a pay-per-view TV) to subscriber system (i.e., provider). The service request comprises IP address of service terminal, identification information of mobile terminal, specifically, a network identification code and a telephone number of the mobile terminal. In order for the subscriber system to let the mobile terminal to get access to the Internet, an identification unit and an authentication unit resided at the subscriber system must authenticate the mobile terminal using either network identification code (e.g. IP address) or telephone number of the mobile terminal. ...Therefore, Nakajima does teach the above feature claimed in claim 1.”
See Advisory Action, Continuation Sheet (PTO 303), lines 3-12.

According to **Nakajima**, when the mobile terminal 105 would like to access the Internet 104 (i.e., access the protected area), the mobile terminal 105 transmits a service request to the subscriber system 103, which includes the authentication unit 210 (also referred to as an identification unit 210 (see paragraph [0038])), to have the authentication unit 210 authenticate the service request (see paragraphs [0037] and [0038]). The service request includes both identification information identifying the service terminal 101 and identification information identifying the mobile terminal 105. Specifically, the service request includes an ID number and the IP address of the service terminal 101 (see paragraph [0027], lines 3-7, and paragraph [0037], lines 4-8), and a network identification code (i.e., a serial number) and the telephone number of the mobile terminal 105 (see paragraph [0028], lines 4-6 and paragraph [0037], lines 8-11).

As described in paragraph [0038] of **Nakajima**, the authentication unit 210 of **Nakajima et al.** authenticates the mobile terminal 105 (i.e., determines whether the mobile terminal is under management of the subscriber system 103) by determining whether the telephone number and the network identification code (i.e., serial number) of the mobile terminal 105, which are included

in the service request, are stored in a subscriber database (see paragraph [0038] and step S303). If the telephone number of the mobile terminal 105 and the network identification code (i.e., serial number) of the mobile terminal 105 included in the service request are stored in a subscriber database, then the mobile terminal 105 is authenticated, and the authentication unit 210 extracts from the service request a service delivery point identification consisting of the ID number and the IP address of the service terminal 101 (see paragraph [0039]).

Thus, unlike the claimed invention, **Nakajima** does not disclose or suggest that the authentication unit 210 “*determine[s] the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area.*” If the **Nakajima** reference were to disclose this feature, then the authentication unit 210 would determine the telephone number of the mobile terminal 105 (considered by the Examiner to correspond to the claimed “unique connection identifier of the second network”) by using the IP address of the Internet 104 (considered by the Examiner to correspond to the claimed “unique identifier of the first network”).

However, unlike the claimed invention, the authentication unit 210 of **Nakajima et al.** does *not use* an IP address to determine the telephone number of the mobile terminal 105. In contrast to the claimed invention, the telephone number of the mobile terminal 105 is used to determine whether the IP address is to be sent to a service gateway 102 as a service delivery point. More specifically, as described in paragraph [0038] of **Nakajima**, the authentication unit 210 of **Nakajima et al.** authenticates the mobile terminal 105 (i.e., determines whether the mobile terminal is under management of the subscriber system 103) by determining whether the

telephone number and the network identification code (i.e., serial number) of the mobile terminal 105 included in the service request are stored in a subscriber database (see paragraph [0038] and step S303). If the telephone number of the mobile terminal 105 and the network identification code (i.e., serial number) of the mobile terminal 105 included in the service request are stored in a subscriber database, then the mobile terminal 105 is authenticated and the authentication unit 210 sends the IP address to a service gateway as a service delivery point (see paragraph [0039]).

Thus, unlike the claimed invention, the IP address in **Nakajima** (considered by the Examiner to correspond to the “unique identifier of the first network”) is simply part of the service request, and is not used by the authentication unit 210 to determine the telephone number of the mobile unit 105 (considered by the Examiner to correspond to the “unique connection identifier of second network”).

Based upon the Examiner’s response in the Advisory Action mailed December 27, 2007, it appears that the Examiner considers the network identification code, which is part of the service request sent to the subscriber terminal 103, to be an IP address (i.e., a unique identifier of a first network) that is used to determine the unique connection identifier of the second network. More specifically, the Advisory Action states “In order for the subscriber system [103] to let the mobile terminal to get access to the Internet, an identification unit and an authentication unit [210] resided at the subscriber system must authenticate the mobile terminal [105] **using either network identification code (e.g. IP address)** or telephone number of the mobile terminal.” [Emphasis added.] See Advisory Action, Continuation Sheet (PTO 303), lines 9-11.

However, contrary to the Examiner's assertion in the Advisory Action, first, the network identification code is not an IP address of a network. As stated in paragraph [0028] of **Nakajima**, the network identification code *is a serial number*. Therefore, the network identification code (i.e., serial number) is not a "unique identifier of the first network." Further, the network identification code (considered by the Examiner to correspond to "the unique identifier of the first network") is not used to determine the telephone number of the mobile terminal (considered by the Examiner to be a "unique connection identifier of the second network"). The telephone number of the mobile terminal is already known, and is part of the service request sent to the authentication unit 210.

Further, **Nakajima** teaches that the mobile terminal 105 is authenticated "by determining whether the network identification code (A) and the telephone number (B) included in the service request are stored in the subscriber database 210D." See paragraph [0038]. Therefore, contrary to the Examiner's assertion, it is clear that **Nakajima** does not use the IP address to perform authentication. As described in paragraph [0038], the IP address does not participate in the authentication (see last four lines of paragraph [0038], and **Nakajima** only sends the IP address to the service gateway 102, after authentication has been performed, to identify a service delivery point (see paragraph [0039]).

Nakajima does not disclose or suggest the claimed "storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit," recited in claim 1

Nakajima discloses that the network identification code (serial number) and the telephone number of the mobile terminal 105 are stored in a subscriber database 210D of authentication unit 210 (see paragraph [0038]). Thus, the authentication unit does not store “a combination of ...the unique connection identifier of the second network [considered by the Examiner to be the telephone number] ... and the unique identifier of the first network [considered by the Examiner to be an IP address].” In other words, the subscriber database 210D does not store a combination of a telephone number and IP address of the mobile phone 105.

In the Advisory Action dated December 27, 2007, the Examiner addresses the above arguments as follows:

In order to authenticate the mobile terminal, the subscriber system must compare the information presented in the service request (i.e., network identification code, telephone number or IP address) of the first and second network) with the stored information at the subscriber system ...”. See Advisory Action, Continuation Sheet, fourth paragraph.

However, the above comments are erroneous in that the IP address in the service request is not compared with the information stored in the subscriber database 210D. Only the network identification code (serial number) and telephone number are compared with information stored in the subscriber database 210D (see paragraph [0038]). Further, the above comments set forth in the Advisory Action do not address the argument that the **Nakajima** reference does not disclose storing “a combination of ...the unique connection identifier of the second network [considered by the Examiner to be the telephone number] ... and the unique identifier of the first network [considered by the Examiner to be an IP address].”

Accordingly, it is submitted that **Nakajima** does not disclose all of the elements of the invention recited in claim 1, as required under §102. Appellants request that the Board reverse the rejection of claims 1-15 and 22-23 under §102 for the reasons set forth above.

The Nakajima reference does not disclose all elements recited in claim 16

Independent claim 16, and claims 17-23 which depend therefrom, are argued as a group with respect to this argument

The Nakajima reference does not disclose or suggest "storage of a combination of the unique identifiers in an authentication unit," as recited in claim 16

First, it is noted that the “unique identifiers” recited in claim 16, the combination of which is stored, are provided by respective networks. (“provision of at least one unique identifier respectively from at least two different networks while a connection to both networks exists, whereby the connection to one of the networks happens by means of the other network”). Thus, it is clear that the stored combination of identifiers comes from different networks. Unlike the claimed invention, Nakajima discloses that the network identification code (serial number) and the telephone number of the mobile terminal 105 are stored in a subscriber database 210D of authentication unit 210 (see paragraph [0038]). In other words, the database 210D stores a combination of identifiers from the same network.

The Nakajima reference does not disclose or suggest "deletion of data from the authentication unit as soon as a connection with at least one of the two networks has ended," as recited in claim 16

The **Nakajima** reference is silent with respect to deleting data from the authentication unit 210 as the subscriber database 210D appears to be permanently stored. Further, **Nakajima** is silent with respect to termination of a connection with a network (i.e., “as soon as a connection with at least one of the two networks has ended”) being a condition upon which data is deleted from the authentication unit 210.

In the final Office Action mailed on August 7, 2007, the Examiner addresses the features recited in claim 16 by asserting “Regarding claim 16, this claim has limitations that [are] similar to those of claims 1 and 5, thus it is rejected with the same rationale applied against claims 1 and 5 above.” See final Office Action, page 7, Item 23. The rejection of claim 5 simply cites paragraphs [0042] and [0043] of **Nakajima** to teach the feature “wherein the combination of data is deleted from the authentication unit as soon as the terminal ends its connection with one of the two networks” recited in claim 5.

However, paragraphs [0042] and [0043] of **Nakajima** relate to sending a bill (invoice) to the mobile terminal by short mail system (SMS) when a session between service terminal 101 and the Internet 104 has ended. Paragraphs [0042] and [0043] of **Nakajima** are completely unrelated to deletion of data from the authentication unit 210, and are completely unrelated to terminating a connection with a network (i.e., “as soon as a connection with at least one of the two networks has ended”) being a condition upon which data is deleted from the authentication unit 210.

Accordingly, it is submitted that **Nakajima** does not disclose all of the elements of the invention recited in claim 16, as required under §102. Appellants request that the Board reverse the rejection of claims 16-23 under §102 for the reasons set forth above.

Application No.: 10/539,506
Art Unit: 1640

Appeal Brief
Attorney Docket No.: 052703

(VIII) CONCLUSION

For the reasons set forth above, appellants request that the Board of Patent Appeals and Interferences reverse the rejection of claims 1-23

If this paper is not timely filed, appellants hereby petition for an appropriate extension of time. The fee for any such extension may be charged to Deposit Account No. 50-2866, along with any other additional fees that may be required with respect to this paper.

Respectfully submitted,

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP



William M. Schertler
Attorney for Applicants
Registration No. 35,348
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

WMS/dlt

(IX) CLAIMS APPENDIX

1. Method for automatically identifying an access right to protected areas in a first network using a unique connection identifier of a second network, comprising the following procedural steps:

dynamic or static assignment of a unique identifier of the first network for a terminal, during or prior to the latter's connection to the first network by means of the second network; storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit;

a provider of the protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area;

authenticating the unique connection identifier of the second network and/or communicating the unique connection identifier of the second network to the provider of the protected area by means of the authentication unit; and

checking whether an access right for the protected area exists for the unique connection identifier of the second network.

2. Method in accordance with claim 1, wherein the combination stored in the current authentication unit contains further data in addition.

3. Method in accordance with claim 2, wherein the additional data has at least one of the following:

the dial-in number into the first network, a user name (login) and a password.

4. Method in accordance with claim 1, wherein the authentication unit is only run temporarily.

5. Method in accordance with claim 4, wherein the combination of data is deleted from the authentication unit as soon as the terminal ends its connection with one of the two networks.

6. Method in accordance with claim 1, wherein the unique identifier of the second network is a call-up number.

7. Method in accordance with claim 1, wherein the protected area includes the provision of an online individual connection identification.

8. Method in accordance with claim 7, wherein an individual connection identification takes place automatically for the unique connection identifier of the second network.

9. Method in accordance with claim 7, wherein, before release of an individual connection identification, a further entry on the terminal is necessary.

10. Method in accordance with claim 9, wherein the further entry includes the entry of an invoice number and/or a customer number and/or a PIN.

11. Method in accordance with claim 1, wherein only authorized services have access to the authentication unit.

12. Method in accordance with claim 1, wherein the protected area includes at least one of the following services:

provision of contents, electronic trade (e-commerce), payment or settlement services and authorized services.

13. Method in accordance with claim 12, wherein with a payment service, the costs arising are automatically invoiced by means of the unique connection identifier of the second network.

14. Method in accordance with claim 1, wherein further data are automatically called up from the terminal and/or further procedural steps are initiated in the protected area using the unique connection identifier of the second network.

15. Method in accordance with claim 1, wherein further personalization of the terminal takes place by entering a PIN.

16. Method for providing data for automatic identification of access rights to protected areas in networks, comprising the following procedural steps:

provision of at least one unique identifier respectively from at least two different networks while a connection to both networks exists, whereby the connection to one of the networks happens by means of the other network;

storage of a combination of the unique identifiers in an authentication unit;

authenticating and/or issuing of one of the unique identifiers when a corresponding enquiry is made regarding another of the unique identifiers; and

deletion of data from the authentication unit as soon as a connection with at least one of the two networks has ended.

17. Method in accordance with claim 16, wherein at least one of the identifiers is an IP number and/or a unique connection identifier of a terminal.

18. Method in accordance with claim 16, wherein it is checked whether the enquiry originates from an authorized place or from an authorized service.

19. Method in accordance with claim 16, wherein the combination stored in the current authentication unit contains further information in addition.

20. Method in accordance with claim 19, wherein the additional data have at least one of the following: a dial-in number into one of the networks, a user name (login) and a password.

21. Method in accordance with claim 16, wherein a call-up number block or a target number block is identified by means of the authentication unit.

22. Method in accordance with claim 1 or 16, wherein the first and second networks are based on different protocols.

23. Method in accordance with claim 1 or 16, wherein the first network is the internet, and the second network is a telephone network.

(X) EVIDENCE APPENDIX

No evidence under 37 C.F.R. §41.37(c)(1)(ix) is submitted.

(XI) RELATED PROCEEDINGS APPENDIX

No decisions under 37 C.F.R. § 41.37(c)(1)(x) are rendered.